



工业园区 专网部署 白皮书



VISIT...

LANZAROTE
Caliente.COM

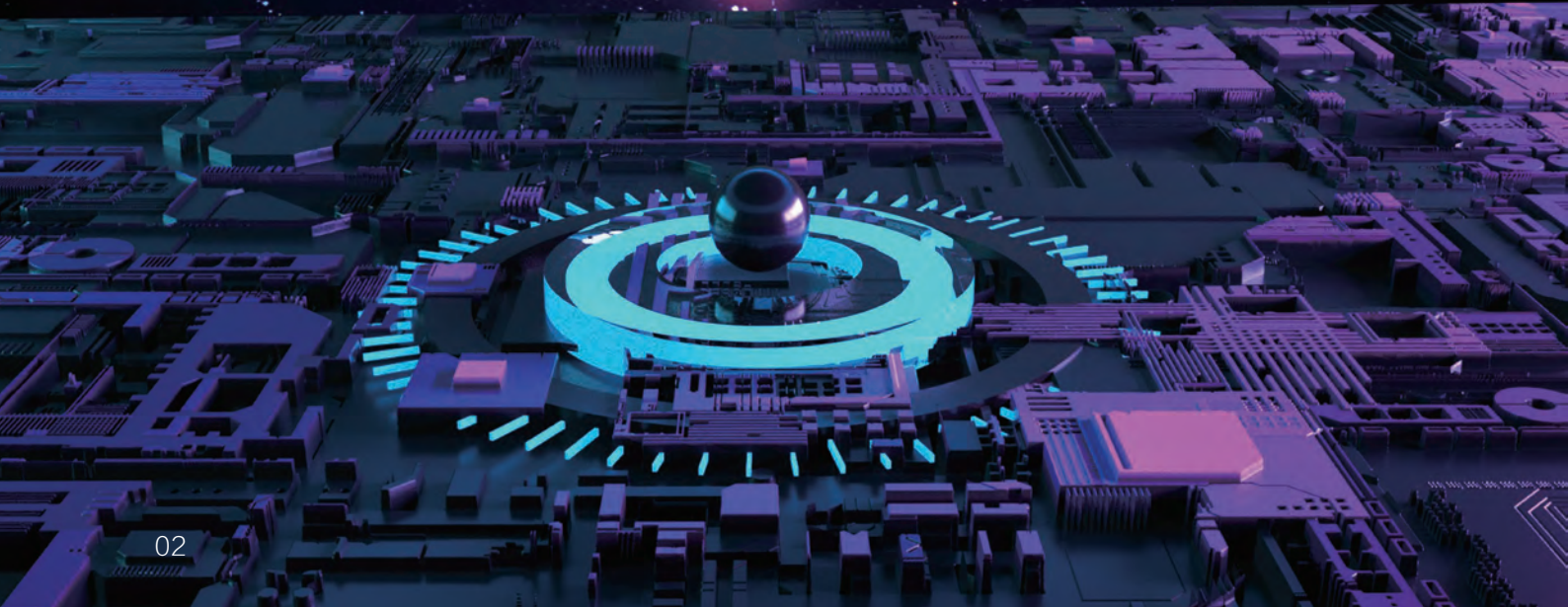
CONTENTS

目录



1. 概述	2
1.1 工业互联网园区网络需求	3
1.2 5G专网的优势	5
1.3 现有5G专网部署方案	6
2. 面向工业互联网园区的5G专网方案	10
2.1 组网模式	11
2.2 组网方案	11
2.3 无线覆盖方案	14
3. 5G定制化能力满足工业互联网园区网络需求	16
3.1 业务隔离与保障方案	17
3.2 5G TSN方案	19
3.3 组通信方案	20
3.4 信息安全方案	22
3.5 定位方案	24
4. 5G专网关键网络产品	26
5. 结束语	28

概述



概述

1.1 工业互联网园区网络需求

工业互联网园区是以高质量发展为目标,按照工业互联网内涵要求,规划、建设、运营、提升的新型园区。根据《工业互联网园区网络白皮书》定义,工业互联网园区网络是指在工业互联网园区内部署的以实现园区企业设备互联和信息互通为目的的网络基础设施,主要由工业生产网、企业信息网、园区公共服务网以及云基础设施组成。其中:

- **工业生产网**是指部署在工厂内部的网络,实现生产现场各类生产设备、传感器、执行器、工控机等互联,以及工业数据采集、工业操控与维护;
- **企业信息网**是指部署在各企业内部的办公区域内的网络,实现部门互通;
- **园区公共服务网**是实现园区内工业企业间互联互通并向园区内各企业提供基础公共服务的网络;
- **云基础设施**为工业互联网园区内部信息汇聚的重要基础设施。

随着社会信息化的发展,信息化对生产效益的促进作用日渐明显,工业互联网园区网络建设成为焦点。工业互联网园区网络需求总结如下:

(1) 无线化需求

工业互联网园区现有部署主要是基于有线网络。在工业控制(现场/远程)场景下,户外挖掘机、室内AGV(Automated Guided Vehicle, 自动导引运输车)等,移动设备无法使用线缆进行连接控制。相较而言,无线网络具有灵活快速布网和低网络维护成本等优势,可以避免有线网络中通信线缆铺设困难、维护成本高、缺乏灵活性等问题。工业互联网园区在室内、外都有无线连续覆盖的需求。

(2) 多类型业务接入需求

工业互联网园区同时存在高带宽、超低时延 & 高可靠性及海量设备等多业务接入场景,需要支持并确保多业务并发下的性能保障。

- **高带宽场景**: 主要用于园区、厂区内的巡检和产品质量检测等领域,如高清视频监控、机器视觉等视频类业务,对网络上行带宽有较高要求,4K 高清视频传输上行速率要求 >25Mbps, 8K 高清视频传输上行速率要求 >100Mbps。
- **超低时延 & 高可靠性场景**: 如自动驾驶、工业控制类业务。自动驾驶需求目前聚焦于工业园区室外摆渡车。工业控制可分为过程控制和运动控制;其中,运动控制对网络要求较高:时延小于 5 ms, 时延抖动为微秒级别,可靠性要求为 99.9999%, 应用场景有大型打印机、数控车床、包装设备等。

- 大连接场景：主要为各种传感器数据的上传，传输的数据量小、连接数多，设备连接密度需求达百万以上 /km²，传输时延要求通常在 50ms 以上。需要注意的是，大规模连接中不同设备的传输需求差异较大，该类业务中基于安全应用的传输时延要求在 10ms 以内。

此外，TSN（Time Sensitive Networking，时间敏感网络）网络目前已成为工业互联网的必选项，旨在为特定的工业互联网应用提供确定性传输服务，确保有界延迟、低延时抖动、低丢包率的报文传输。时延抖动要求控制在一定范围内，通常为纳秒级。工业互联网园区网络需要支持 TSN 技术。

（3）安全需求

安全是工业界最关注的问题，保障工业网络不受入侵、工业数据不被窃取是工业网络构建的基本要素。对于工业互联网园区而言，数据不出园区通常是一个最基本的安全需求。此外，对于一些有极高安全需求的场景，如某些特殊企业的工业制造园区，由于生产信息属于非常高级别的保密信息，因此需要符合特定安全保密规定，定制开发特定的加密算法，提供安全保障。

（4）异构终端接入管理和多协议互通的需求

在工业现场，机器设备类型和设备接口多样化。工业互联网园区网络需要支持多方式接入，包括 3GPP 无线网络接入和 Wi-Fi、ZigBee 等无线接入方式，以及以太网、光纤、各类工业总线等有线接入方式。

（5）园区内外交互业务需求

工业互联网园区网络需要支持不出园区业务和广域业务两种业务交互场景。其中，广域业务场景要求行业终端能够从工业园区专网接入运营商公网，也可以从运营商公网接入工业园区专网。

（6）组通信需求

组通信可以实现一个组内的成员之间的相互通信，支持一个组成员与其他多个组成员之间的组播数据路由或者广播数据路由。工业互联网园区的一些应用场景对组通信有实际需求。例如，电力领域中的智能分布式 FA（Feeder Automation，馈线自动化）业务，其核心思想就是通过相邻智能配电终端之间的对等通信层收集故障信息，基于终端设备间的报文组播转发进行故障诊断和隔离，通过去中心化实现信息的快速交互，实现毫秒级的供电不间断。



（7）定位需求

工业互联网园区内的移动类业务，如移动机器人等，除了对网络时延、网络覆盖、切换有要求外，还对精准定位有较高要求。此外，工厂环境对室内定位的需求也日益强烈，很多应用离不开室内定位技术，如人员的定位监控、设备的定位监管以及安全预警管理等。

（8）自主运营管理需求

工业互联网园区网络的使用、维护和运营可以由部署网络的企业负责，企业对园区专网具有自主的掌控和维护能力，包括设置专用的用户数据库，对用户信息进行管理，以及培养专用的运维管理人员、建设专用的网络运营平台等。

1.2 5G 专网的优势

5G 凭借大带宽、低时延 & 高可靠性、海量连接等技术特性以及在网络架构上的灵活性，高度契合专网的需求。相比传统专网如 Wi-Fi 接入技术，主要优势体现在良好的网络覆盖性、双向认证的安全性、更快的速度和更低的延时抖动、移动业务的连续性等方面，具体如表 1 所示。

表 1 5G 专网的优势

优势项	说明
容量和覆盖	大容量 广覆盖
技术演进	全球范围的标准演进，提供 5G 网络定制化能力
性能	提供工业级的可靠性 提供超低时延传输、有界传输时延和低时延抖动
业务质量	通过网络切片提供业务隔离 提供基于流的 QoS 保障和优先级机制
安全性	可提供电信级别的安全性
移动性和定位	5G 基于 3GPP 标准规范，天然的无缝移动通信机制 支持室外与室内定位无缝覆盖

1.3 现有 5G 专网部署方案

面向行业用户的 5G 专网部署方案分为四种：基于端到端网络切片的虚拟专网方案、专网与公网之间 RAN（Radio Access Network，无线接入网）和核心网控制面共享方案、专网与公网之间 RAN 共享方案和基于物理隔离的独立专网方案。

（1）基于端到端网络切片的虚拟专网方案

该方案中，行业用户无需部署任何 5G 网络设备，专网和公网端到端共享运营商 5G 基站和核心网全套设备，如图 1 所示。方案的优点在于成本低，行业用户无需投资任何建设成本，只需向运营商订购网络切片服务就可实现专网功能；缺点在于 UPF（User Plane Function，用户面功能）部署在运营商侧，不能满足数据不出园区的要求。该方案同时适用于局域场景及广域场景，主要面向对网络性能要求不高和成本敏感的行业用户。这里需要说明的是，现阶段网络切片在技术、标准和产品成熟度方面还无法提供完善的可商用端到端解决方案。

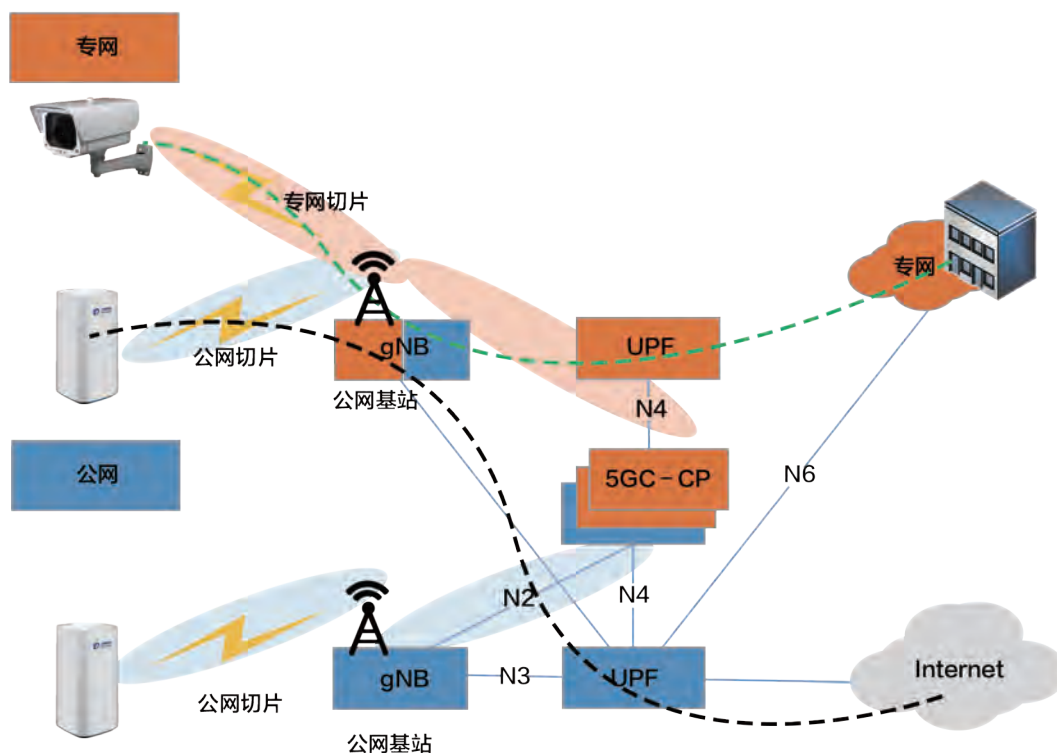


图 1 基于端到端网络切片的虚拟专网方案

（2）专网与公网之间 RAN 和核心网控制面共享方案

该方案中，行业用户只需部署核心网用户面设备，专网和公网共享运营商 5G 基站以及核心网的控制面设备，如图 2 所示。相比虚拟专网方案，该方案成本较高，适用于局域场景；同时由于 UPF 部署在企业园区，可以保证专网数据流量的安全性。此外，从目前产业界情况来看，核心网 N4 接口的解耦工作进展迟缓，不同厂家的核心网控制面设备和 UPF 之间难以实现互联互通。因此，采用该方案进行 5G 专网建设存在着被公网核心网设备厂商绑定的问题。

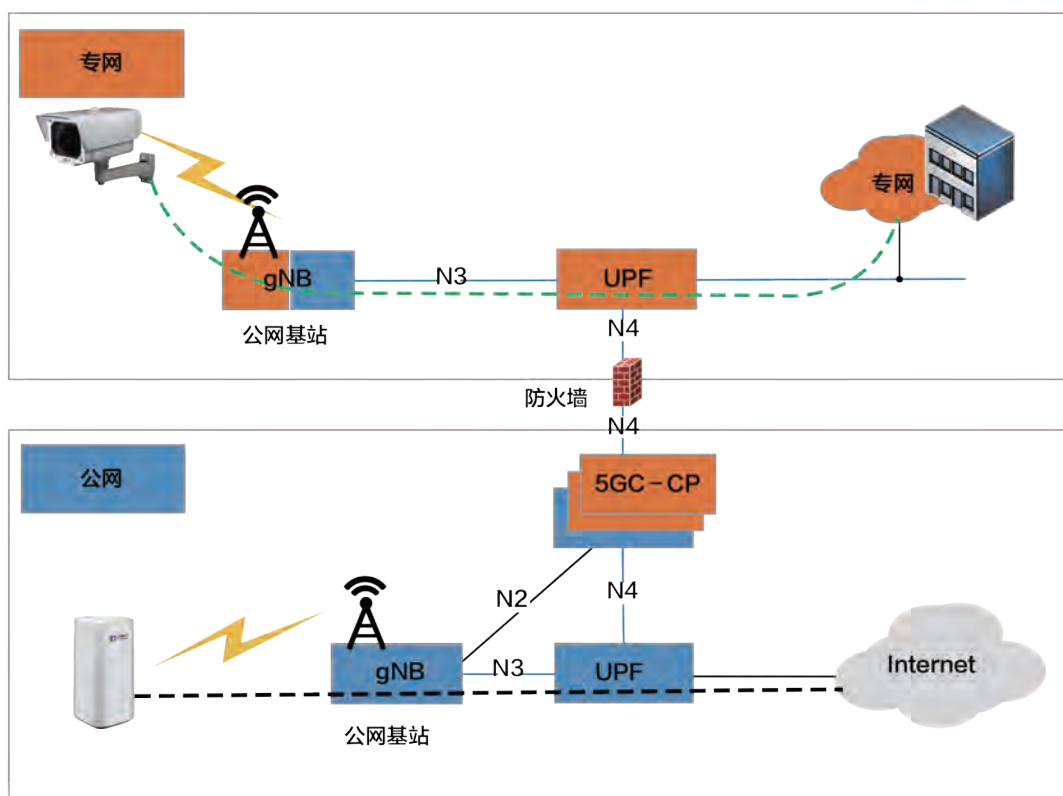


图 2 专网与公网之间 RAN 和核心网控制面共享方案

工业园区 5G 专网部署 白皮书

（3）专网与公网之间 RAN 共享方案

该方案中，行业用户新建部署 5G 核心网设备，包括核心网控制面设备和 UPF，专网和公网在无线网侧共享 5G 基站，如图 3 所示。同专网与公网之间 RAN 和核心网控制面共享方案类似，该方案也是与公网混用方案，但不涉及核心网 N4 接口开放的问题。

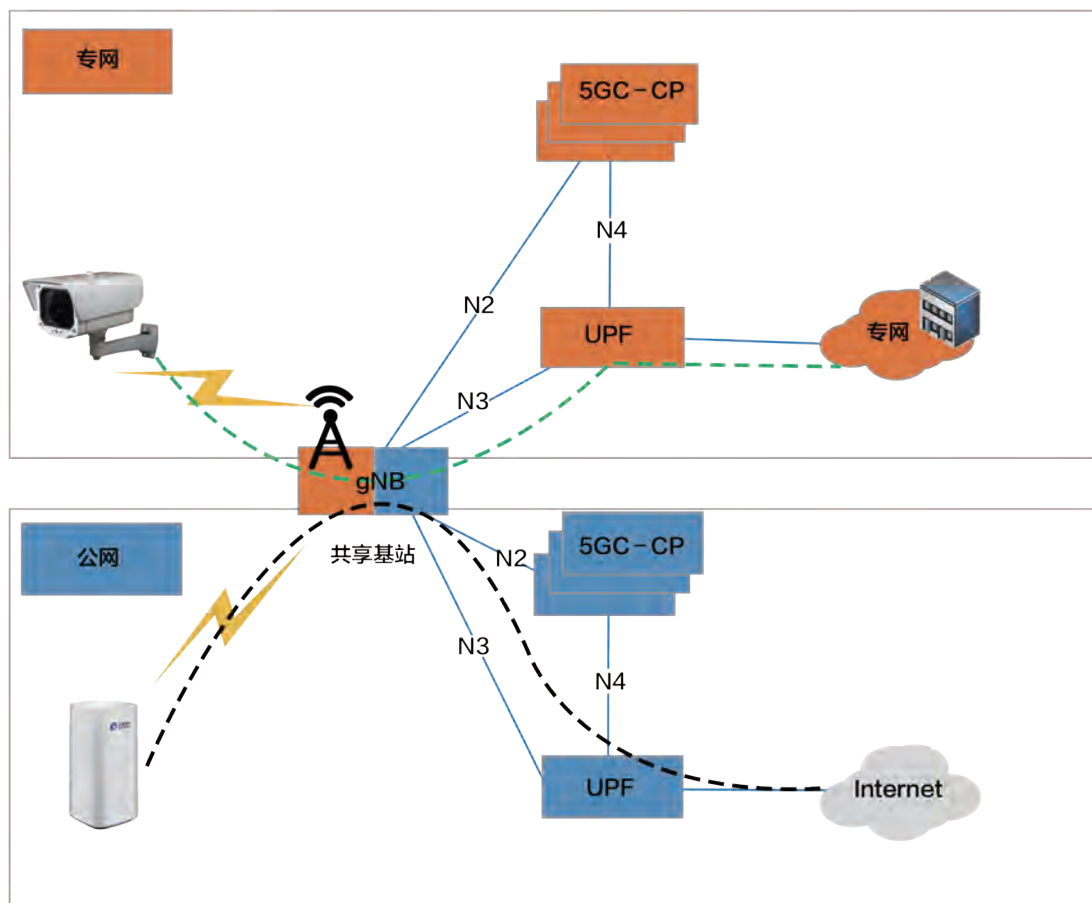


图 3 专网与公网之间 RAN 共享方案

（4）基于物理隔离的独立专网方案

该方案中，行业用户自行部署全套 5G 网络设备，包括专用的无线网和核心网，所有行业终端的控制面和用户面数据都承载在独立专网上，如图 4 所示。由于专网和公网物理隔离，因此，可提供完整的数据安全性，保证企业内部数据不外泄。同时，行业用户具有网络自主掌控权，可以实时按需调整网络、管控终端，不受运营商公网影响。相比上述三个方案，该方案的网络建设成本最高。该方案适用于局域场景，主要面向对安全隔离性和网络性能有极高需求的行业用户。

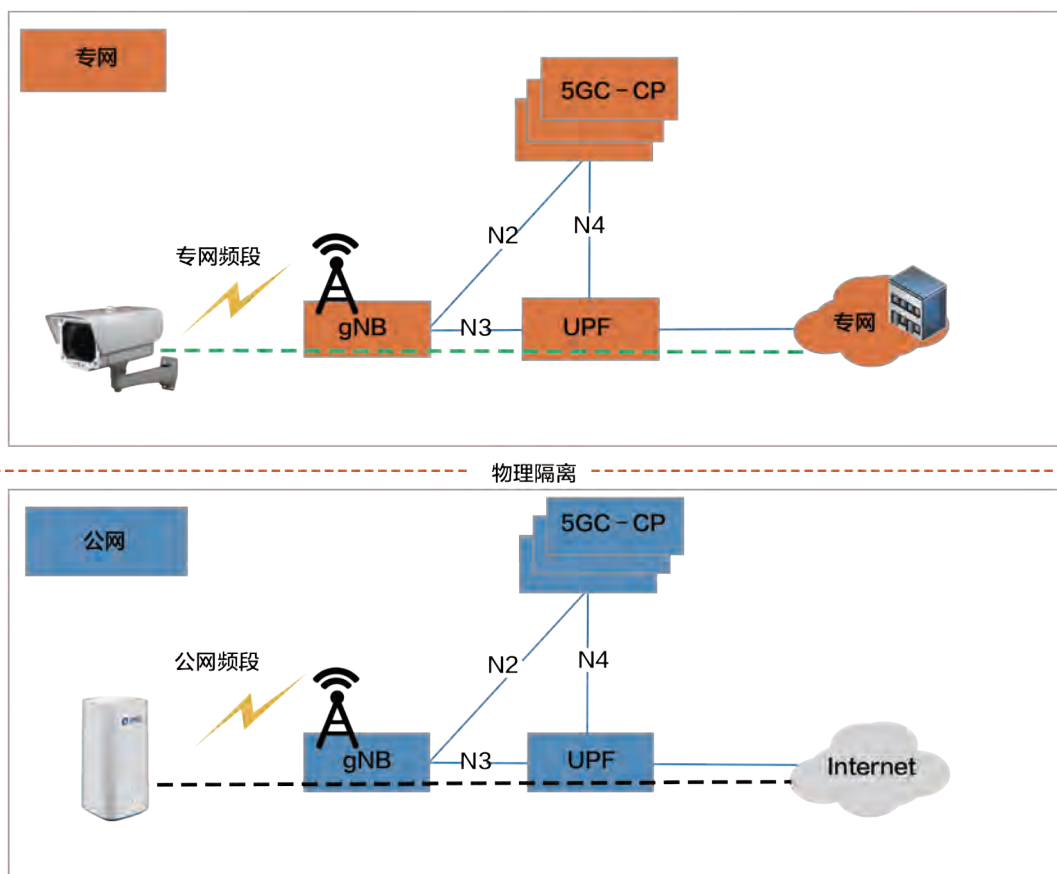
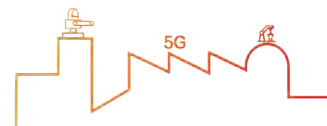


图 4 基于物理隔离的 5G 独立专网方案

总之，不同的场景需求使用不同的解决方案来匹配解决。选择部署方案时，需要综合考虑行业用户在成本、安全性、业务性能和业务连接范围等方面的需求。

面向工业互联网园区 的 5G 专网方案



面向工业互联网园区的 5G 专网方案

2.1 组网模式

5G 网络架构分别为 NSA（Non-Standalone，非独立组网）和 SA（Standalone，独立组网）两种模式。其中，SA 是 5G 网络演进的终极目标。相比 NSA 网络，SA 网络复杂度低，终端实现简单；并且，能同时支持 eMBB（Enhanced Mobile Broadband，增强移动宽带）、uRLLC（Ultra-reliable and Low Latency Communications，超高可靠与低时延通信）、mMTC（Massive Machine Type Communication，大规模机器类型通信）等多种应用场景。此外，当前 SA 产业成熟度也可以满足建网要求。因此，面向工业互联网园区的 5G 专网建设建议采用 SA 网络架构。

2.2 组网方案

工业互联网园区出于对网络安全、管理控制的极高要求，需要建立一张与公网隔离的独立网络。然而，现有的独立专网方案中，公网与专网之间物理隔离，不能满足终端从专网接入公网或者从公网接入专网的使用需求。为此，引入 NPN（Non-Public Network，非公共网络）技术应用于工业互联网园区的方案部署。NPN 提供了两种部署方式：SNPN（Standalone NPN，独立 NPN）和 PNI-NPN（Public network integrated NPN，公共网络集成 NPN），这两种方式都可以和工业互联网进行很好地融合，其区别在于 SNPN 网络不依赖于公网，由 SNPN 运营商运营，而 PNI-NPN 网络依赖于公网，由传统运营商运营。考虑到园区企业运营的自主性以及功能按需定制的灵活性，建议在工业互联网园区采用 SNPN 方式建立 5G 专网，为园区内所有终端设备提供通信服务。**5G 专网主要由终端设备、基站设备、MEC（Multi-access Edge Computing，多接入边缘计算）设备、核心网设备以及网络管理平台等组成。**

- 终端设备主要包括手持 5G 智能终端、5G 通信模组、5G 无线网关设备等。其中，手持智能终端设备为园区管理人员、生产工作人员提供生产信息查询、设备操作、定位、图像和数据传输等功能；5G 通信模组主要安装在各类传感器、便携式移动设备和采集设备上，支持数据传输、定位等功能；5G 无线网关部署在工业现场，对工业现场各种机器和设备接口进行统一的管理，提供综合接入基站的能力，网关支持以太网口、Wi-Fi、蓝牙和 RS232/485 等主流协议，实现园区内异构网络的管理连接。

工业园区 5G 专网部署 白皮书

- 基站设备提供 5G 专网覆盖，实现管理人员及园区内各类无线宽带终端的接入功能，为覆盖区域内的终端提供无线资源分配和调度、移动性管理等功能，满足无线覆盖区域内宽带移动用户的通信保障需求。
- MEC 设备为园区内提供专用 MEC 服务环境，其上部署工业互联网内相关的所有上层应用，如工业控制应用、位置应用等。
- 核心网设备实现对基站的控制和管理，提供用户的鉴权、接入、业务连接、数据管理等功能。
- 网络管理平台用于管理相关的网络层设备，包括服务器、操作维护终端、告警终端、告警箱、管理控制台以及一些组网设备。

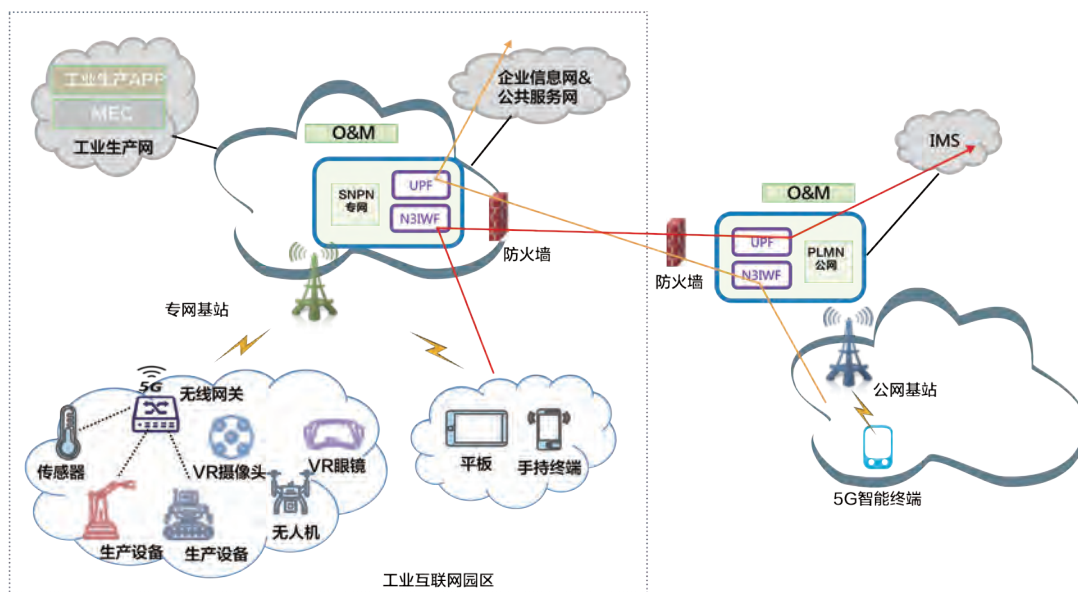


图 5 工业互联网园区 SNPN 独立专网组网方案



如图 5 所示，SNPN 网络与公网相互隔离，核心网之间没有控制面接口，不能进行互操作。SNPN 的用户签约数据、控制面流量和用户面流量均保持在 SNPN 网络内。对于园区内部的数据交互，通过 SNPN 专网 UPF 设备本地终结，保证数据不出园区。SNPN 重用了“Untrusted non-3GPP access”架构，保证专网终端设备可以通过 SNPN 专网的用户面访问公网业务，或者通过公网的用户面访问 SNPN 专网业务。具体为：

- 对于园区内有访问公网业务需求的终端，可签约运营商的 PLMN（Public Land Mobile Network，公众陆地移动网）服务，通过 SNPN 专网的 UPF 连接公网的 N3IWF（Non-3GPP InterWorking Function，非 3GPP 互通功能），实现对公网业务的访问。数据路径参见上图中红色线标识。

- 对于园区外访问内网业务的终端，可通过公网对接 SNPN 的 N3IWF 实现。数据路径参见上图中黄色线标识。

针对工业互联网园区的一些个性化应用，行业终端、基站和核心网需要具备定制化能力。具体为：

- 针对三大典型应用场景，行业终端和基站需要支持灵活的帧结构配置，以及诸如上行增强、重复传输等特性。进一步地，对于确定性时延应用场景，核心网和终端需要支持 TSN 能力。

- 网络切片用于工业互联网园区内不同应用场景的安全隔离和业务保障，要求终端设备具备感知切片与匹配切片的能力；基站能够通过无线参数或算法配置保障切片级的 QoS（Quality of Service，业务质量）需求；核心网能够按需提供资源隔离能力等。

- 针对组通信需求场景，核心网需要支持组管理功能和虚拟 LAN（Local Area Network，局域网）内终端之间的组播机制。

- 针对信息安全增强场景，特别是面向某些特殊企业的工业互联网园区，由于生产信息涉及非常高级别的保密信息，因此需要引入特定密码系统，通过定制终端和核心网安全功能，保障终端接入安全和应用安全。

- 室内定位场景下，5G 网络与 BLE（Bluetooth Low Energy，低功耗蓝牙）融合部署，要求分布式 Pico RRU（Radio Remote Unit，射频拉远单元）集成蓝牙信标管理网关、室分吸顶天线内置蓝牙信标等功能。

参见第 3 节描述。

2.3 无线覆盖方案

国内目前无 5G 行业专用频段，且短期内 5G 行业频率不够明朗。因此，面向工业互联网园区的 5G 独立专网建设，只能考虑租用运营商频谱的方式。由运营商统一规划，为其分配授权频谱中的企业独占频段。

工业互联网园区 5G 网络信号覆盖方案按照室外区域和室内区域两方面进行建设。

- 室外区域建设主要实现广域打底覆盖，尽量采用低频段，如可采用 700M 4TR RRU（中国移动）或 2.1G 4TR RRU（中国电信、中国联通）。针对室外大容量高速率场景，需要使用大带宽和大规模天线技术，可采用 64 通道产品，如 2.6G 64TR AAU（Active Antenna Unit，有源天线单元）（中国移动）或 3.5G 64TR AAU（中国电信、中国联通）。此外，在宏站弱覆盖以及热点区域可以采用微站或杆站进行补盲补热。

- 室内区域建设主要面向工业生产网生产车间以及企业信息网办公区域等。考虑到室内对设备体积要求较高，因此不宜用大规模天线部署。在容量要求高的热点覆盖区域，可以采用高频超密集组网，如采用 4TR pRRU 数字化室分系统。

工业园区的一些应用对于上行速率和时延有较高要求，且需要连续移动作业，如远程驾驶控制等。由于在切换时会发生速率和时延波动，这种不稳定的传输性能可能导致业务感知的急剧下降，影响业务效果。在这种场景下，可以使用融合高低频的双频网络，如 2.6G+4.9G 双频网络（中国移动），使终端可以在高频站和低频站中错峰切换，双频协同保证稳定的上行高速率，以有效解决单频网络下基站切换期间速率下降的问题，保障良好的业务感知。



面向工业互联网园区的 5G 专网方案

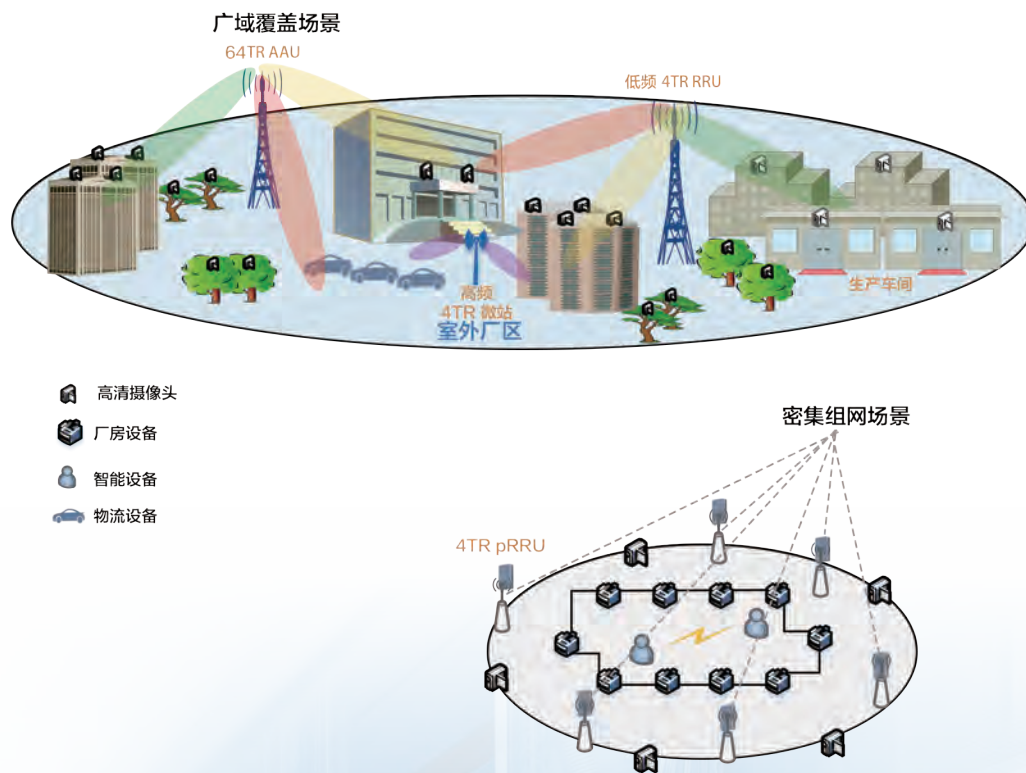


图 6 工业互联网园区无线覆盖示意图

5G 定制化能力满足工业 互联网园区网络需求



3.1 业务隔离与保障方案

工业生产网内部同时存在着各类生产相关的业务应用，涉及 eMBB、uRLLC、mMTC 等三大业务场景，如控制系统产生的控制指令、数据采集系统产生的传感器数据、监控系统产生的音视频文件等，需要从架构设计上考虑资源的隔离及算法的协调，确保并发场景下的业务性能保障。

图 7 工业互联网园区业务隔离方案

网络切片提供切片间的资源隔离。在工业互联网园区，**主要包括核心网切片的资源隔离和接入网切片的资源隔离。**

从资源视图的角度看，核心网切片的资源隔离主要涉及硬件资源层、虚拟资源层和网元功能层。其中，硬件资源层主要指基于 X86 或者 ARM 架构的各种服务器；虚拟资源层主要对应网络功能虚拟化基础设施（NFVI，Network Functions virtualization Infrastructure），通过虚拟机、容器等虚拟化技术，在通用硬件上承载传统通信设备功能的软件处理。网元功能层主要指核心网的虚拟网络功能（VNF，Virtual Network Function）。

- 从**硬件资源层**上，工业生产网与企业信息网、公共服务网之间使用不同的硬件资源，进行物理隔离，保证工业生产网资源独占，不受外部影响。

- 从**虚拟资源层**上，工业生产网中的各类业务场景之间逻辑隔离，企业信息网和公共服务网之间逻辑隔离。基于虚拟机或容器的隔离机制，各切片使用不同的虚拟资源池，保证不同切片间的业务独立性。

- 从**网元功能层**上，工业生产网三类业务场景切片之间以及企业信息网和公共服务网切片之间，采用 AMF（Access and Mobility Management Function，接入和移动管理功能）与 UDM（Unified Data Management，统一数据管理设备）网元功能共享、SMF（Session Management Function，会话管理功能）与 UPF 网元功能独占专享的方式构建，同时，工业生产网与企业信息网和公共服务网之间设置独立的数据库。

在工业生产网切片中，考虑到三类场景业务需求差异化显著和高质量的业务保障要求，在无线上，切片间采用基于逻辑小区的隔离方式。不同切片使用不同的载波小区，每个切片仅使用本小区的空口资源，切片间严格区分，以确保各自的无线资源。这样做的好处是，可以根据业务需求对小区进行定制化配置（如帧格式配置）或进行专门的空口侧优化等。具体为：

- 对于 eMBB 切片，采用较小的子载波间隔和为小区配置更宽的载波带宽，实现更高速率的数据传输和满足更高的容量需求。上行容量要求较高时，可以采用灵活的帧结构，如 3:1 的上下行子帧配比，增强上行能力，承载更高的回传数据。此外，还可以采用超级上行方案，通过 TDD 和 FDD 的协同、高低频的互补、时域和频域的聚合，提升上行带宽和增强上行覆盖。

- 对于 uRLLC 切片，由于要求提供毫秒级的端到端时延和接近 99.999% 的业务可靠性保证，可以采用较大的子载波间隔和引入短传输时隙，实现低延迟通信需求。通过使用低谱效的 MCS（Modulation and Coding Scheme，调制与编码方案）和分集、冗余技术等实现高可靠性。

- 对于 mMTC 切片，重点关注终端节电（包括连接态和空闲态）、通过重复传输方式进行覆盖增强，以及增强的随机接入和合适的拥塞控制等方案的应用。

企业信息网切片和公共服务网切片之间共用同一个小区的 RB（Resource Block，资源块）资源，按 QoS 优先级进行业务保障。同时，可以根据各切片的资源需求，为特定切片预留分配一定量的 RB 资源。预留策略也比较灵活，如静态预留，这部分预留的资源在任何时刻都不能被其他切片用户使用；或动态预留，为指定切片预留的资源在该切片不需要使用时，可以被其它切片用户使用。针对这两个网络切片，需要差异化配置切片上下行最大资源、切片上下行保障资源和切片接入的最大用户数等参数，一方面用于切片业务质量的保障，另一方面，限制某个切片对共享资源过度使用，影响到另一切片。

除了切片间的资源隔离外，针对具有极高数据安全要求的场景，还可以采用独立的切片内数据面密钥方案，提供可靠的数据隔离能力。

3.2 5G TSN 方案

在工业互联网园区，存在着大量对时间非常敏感的应用，如运动控制、机器人协同控制等。这些应用的数据需要在确定时限内发送到目标，以支持工控设备和应用的正常运转。TSN 是一种具有有界传输时延、低传输抖动和极低数据丢失率的高质量实时传输网络。利用 TSN 网络可以满足工业应用控制信息和运维数据的时间敏感传输要求。

传统 TSN 网络基于通用的以太网标准来建设，是一种有线通信的网络，各类工业设备（如传感器、执行器等）都需要以有线方式连接到 TSN 网络，终端设备之间以及终端设备与云平台之间的数据交互会受电缆布线的限制。5G 技术与传统 TSN 网络无缝融合，可以实现 TSN 网络的无线化。

相比 uRLLC 技术在可靠性和时延方面的保障，5G TSN 技术进一步地在时延抖动和时间同步方面对 5G 网络进行增强。5G 核心网在 uRLLC 通信服务基础上增加了时间同步、时延和时延抖动有界性，增强了可靠性指标。

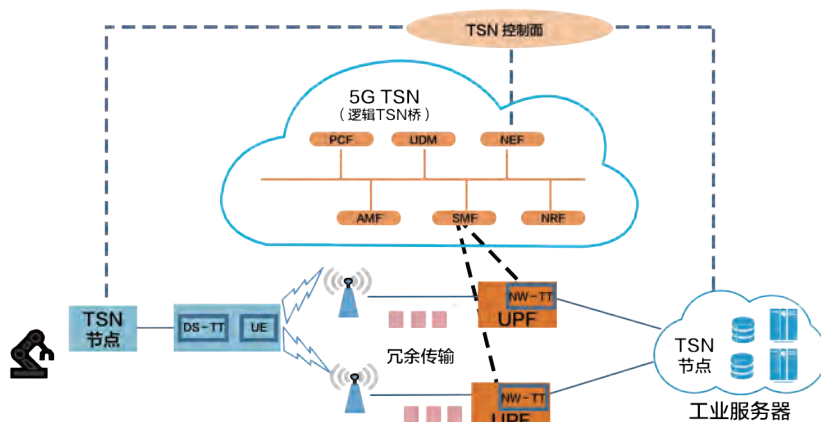


图 8 工业互联网园区 TSN 网络无线化方案

5G TSN 架构如图 8 所示。图中，5G 网络作为 TSN 的一个节点，充当 TSN 桥，集成在 TSN 系统中。此逻辑 TSN 桥包括了 UPF 的 NW-TT（Network-side TSN translator，网络侧 TSN 翻译器）端口、UE 和 UPF 之间的用户面隧道，还有 UE DS-TT（Device-side TSN translator，终端侧 TSN 翻译器）端口。通过冗余用户面路径实现可靠的数据传输。

5G TSN 技术对终端和核心网均有定制化要求。终端和 UPF 需要支持 TSN Translator 功能，核心网通过能力开放与 TSN 系统控制面功能进行对接，完成协议解读和参数映射。在工业互联网园区网络中，TSN 系统控制面功能可以部署在 MEC 平台上。

3.3 组通信方案

5G LAN（5G LAN-type service，5G 本地局域网类型服务）技术首次在移动网络中引入终端组管理的概念，支持组内终端直接通信。组通信方案的主要技术特征有：

- 组管理包括组标识、组成员和组数据管理。其中，组标识用于识别一个组；组成员可用 GPSI（Generic Public Subscription Identifier，通用公共用户标识）list 表示，每个 GPSI 唯一标识一个组成员；组数据则是组通信对应的 PDU（Protocol Data Unit，协议数据单元）会话信息，包括 PDU 会话类型（IPv4、IPv6 或者以太网类型）、DNN（Data Network Name，数据网络名称）、S-NSSAI（Single Network Slice Selection Assistance Information，单个网络切片选择辅助信息）和应用标识符。
- 组管理包括两种方式：静态组管理和动态组管理。其中，静态组管理方式中，组信息由 O&M 触发创建、删除、更新；动态组管理方式中，组信息通过核心网能力开放接口动态配置或调整。
- 组通信可以发生在组内的两个成员之间或者多个成员之间，不同组之间通信隔离。
- 支持根据组成员的位置限制其组成员的通信。
- 通过核心网能力开放接口，可以定制终端设备的 IP 地址分配策略、流量路由策略等。
- 5G LAN 只涉及核心网功能，对终端和基站无影响。

在工业互联网场景下，可通过构建不同的 5G LAN 群组，实现不同等级终端之间的安全隔离。如图 9 所示。

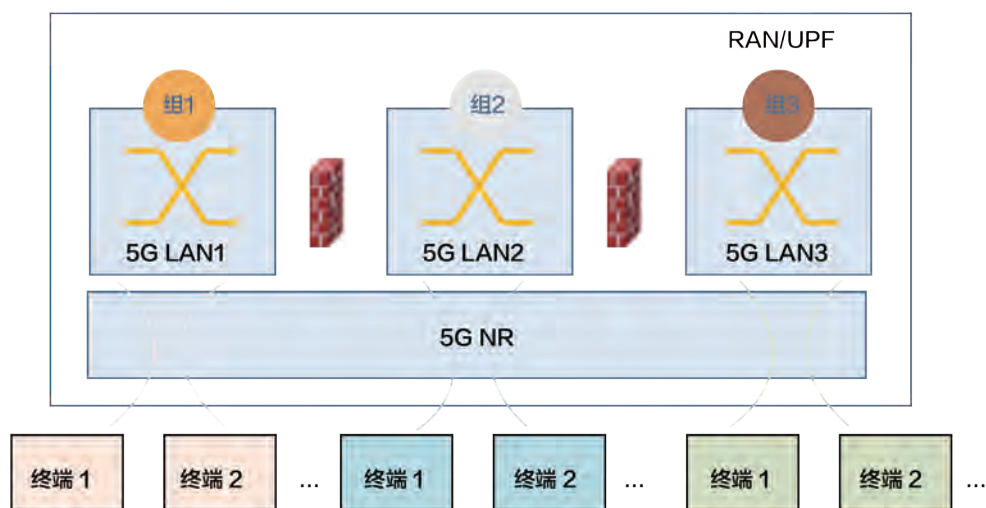


图 9 工业互联网园区组通信隔离示意图

对于工业互联网园区内有组通信需求且有极高安全需求的区域（如生产区），可以通过配置 5G LAN 组的可用地理区域，限制 5G LAN 的组通信，如图 10 所示。当组成员移出该区域时，不能发起到对应 5G LAN 的组通信，以此保证通信安全。

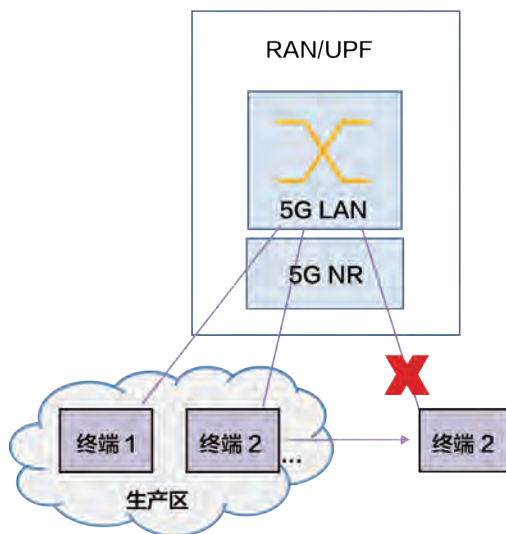


图 10 工业互联网园区组通信限制示意图

对于工业互联网园区内有跨区域（如多个生产车间之间）组通信需求的场景，可以通过静态 IP 地址分配方式，为组内终端指定 IP 地址。由于组内的终端可以配置为相同的地址段，因此，可以在一个更广覆盖范围下实现局域网内的相互通信，如图 11 所示。

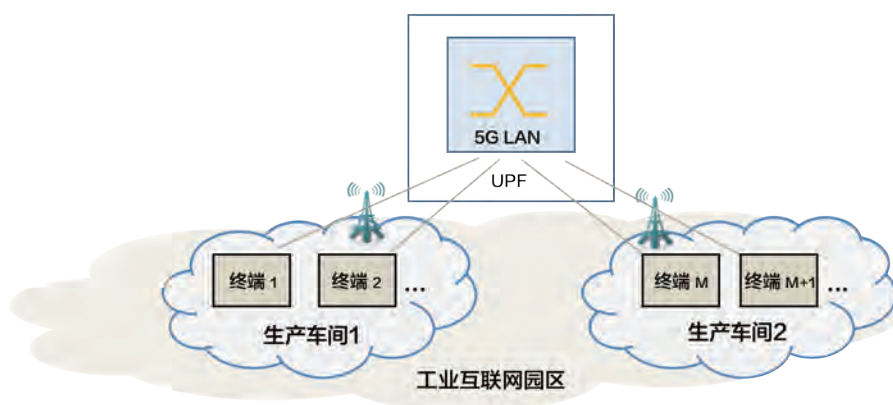


图 11 工业互联网园区跨区域组通信示意图

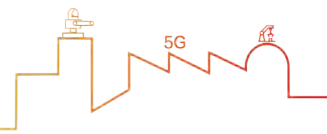
3.4 信息安全方案

参考 3GPP 安全架构，5G 专网可以划分为 4 个域：接入域、网络域、业务域和管理域。其中，接入域包含终端和基站设备；网络域是 5G 核心网；管理域为 5G 基站和核心网的网管及运营支撑系统；业务域包含工业互联网园区各业务系统。网络的信息安全方案包括以下几个方面：

（1）网络接入安全

基于 5G AKA（5G Authentication and Key Agreement，5G 认证与密钥协商）安全认证机制对终端进行身份认证，确保只有合法的终端能够接入 5G 网络。接入认证的同时，5G AKA 机制能够为终端及网络协商出加密及完整性保护密钥，在网络接入层面和非接入层面对终端信令及用户数据进行加密和/或完整性保护，防止用户信息被篡改、窃听。

使用外部数据网络对终端进行二次认证，防止终端被窃取导致的非法访问。当前的行业终端主要采用无线网关，如 CPE（Customer Premise Equipment，客户终端设备）。CPE 通常位于无人值守的户外，其所使用的 USIM 卡可能被攻击者窃取，然后插入其他设备中冒充正常 CPE 接入移动网络发起网络攻击。二次认证是在终端与 5G 网络之间的双向认证之后，与业务网络之间执行的附加认证，采用 EAP-



AKA (Extensible Authentication Protocol-Authentication and Key Agreement, 可扩展认证协议认证与密钥协商) 认证方式。

(2) 网络域安全

保障网络节点安全、网络节点之间消息传输安全, 解决 5G 核心网虚拟化和服务化架构开放性引入的安全问题, 保证核心网系统可信、可靠运行。通过采用可信服务器增强物理安全, 主机系统加固提升软件系统的安全。通过负荷分担、多点部署、故障检测和恢复, 实现核心网设备 99.999% 的可靠性。通过核心网网元的认证和传输层安全, 保证网元之间的可靠通信。

(3) 业务域安全

保证应用的安全, 解决业务报文在空口、基站、核心网和业务系统之间的传输安全, 防止业务报文被窃听和篡改。在终端业务访问时候, 可以按需建立 IPSec (IP Security, Internet 协议安全性) /SSL (Security Socket Layer, 安全层) VPN 隧道, 保证数据传输安全。

(4) 管理域安全

网管系统与接入网和核心网之间通过防火墙或者网闸进行隔离。

对于生产信息涉及非常高级别的保密信息的工业互联网园区, 如某些特殊企业的工业制造园区, 需要进行信息安全增强。在采取 5G 网络传输工厂生产数据和采集信息时, 其信息传输的安全性应符合某些特殊企业对涉密信息的传输要求, 系统所采用的终端设备应支持某些特定安全保密规定, 保证数据的安全性。为了提升终端与网络之间的安全性, 抗击来自无线接口的攻击, 需要定制终端和增加符合特定标准的特定密码系统。定制终端采用安全芯片为终端提供安全配置、数据加密、安全存储、密钥管理和数字签名等安全功能。高级密码系统生成安全参数, 并基于安全参数推演出用于加密和完保的密钥, 提供安全等级更高的网络, 如图 12 所示。

- 在高级密码系统保存终端的根密钥信息, 保障专网终端在开户过程中无根密钥泄露的风险。
- 由高级密码系统完成所有鉴权向量的生成, 使用符合由高级密码系统完成所有鉴权向量的生成, 使用符合特定标准要求的专用安全算法替换 3GPP 标准协议中的安全算法。标准的专用安全算法替换标准协议中的安全算法。
- 定制化核心网安全功能。在终端接入鉴权过程中, 增加与高级密码系统的交互过程, 相关接口为私有接口。
- 在业务传输路径上, 建立定制终端和高级密码系统之间端到端的传输隧道, 业务报文采用全报文加密, 包括 IP 头, 加密之后的密文在隧道中传输。

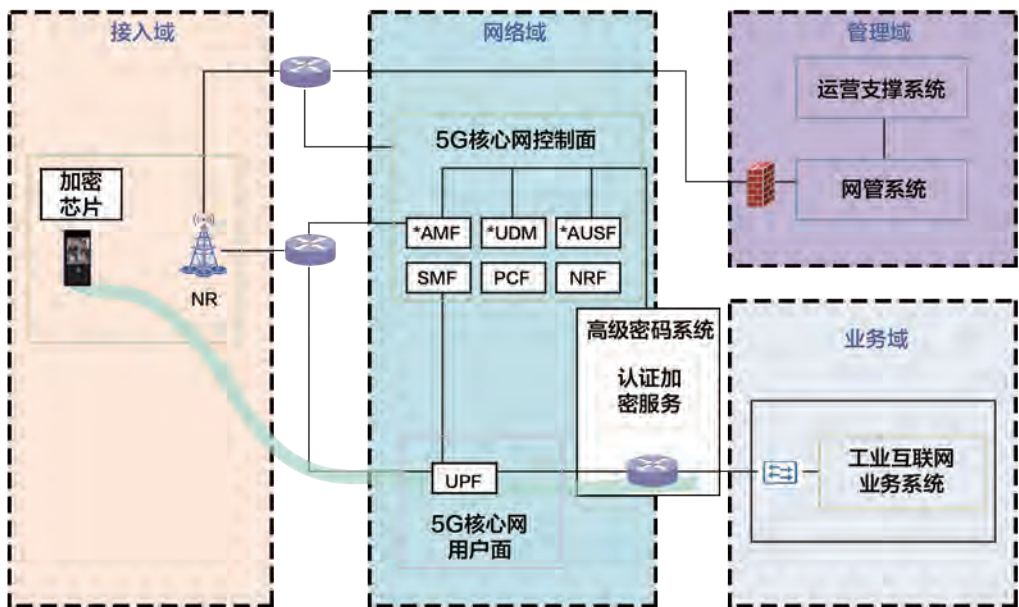


图 12 信息安全增强方案

3.5 定位方案

工业互联网园区的很多业务场景对室内外定位都有强烈的应用需求。5G 网络与传统定位技术的融合，可以实现高精度定位和室内外一体化的无缝定位，满足工业场景的定位需求，同时，还可提供有效的防护机制，保障工业信息的安全性。

5G 网络和基于卫星的无线定位技术结合，可以满足室外定位需求；与基于 BLE 的室内定位系统融合部署，可以在 5G NR（New Radio，新空口）无线覆盖基本功能的基础上，实现室内定位网络的同步建设。图 13 为内置蓝牙信标系统的室内融合型组网方案。

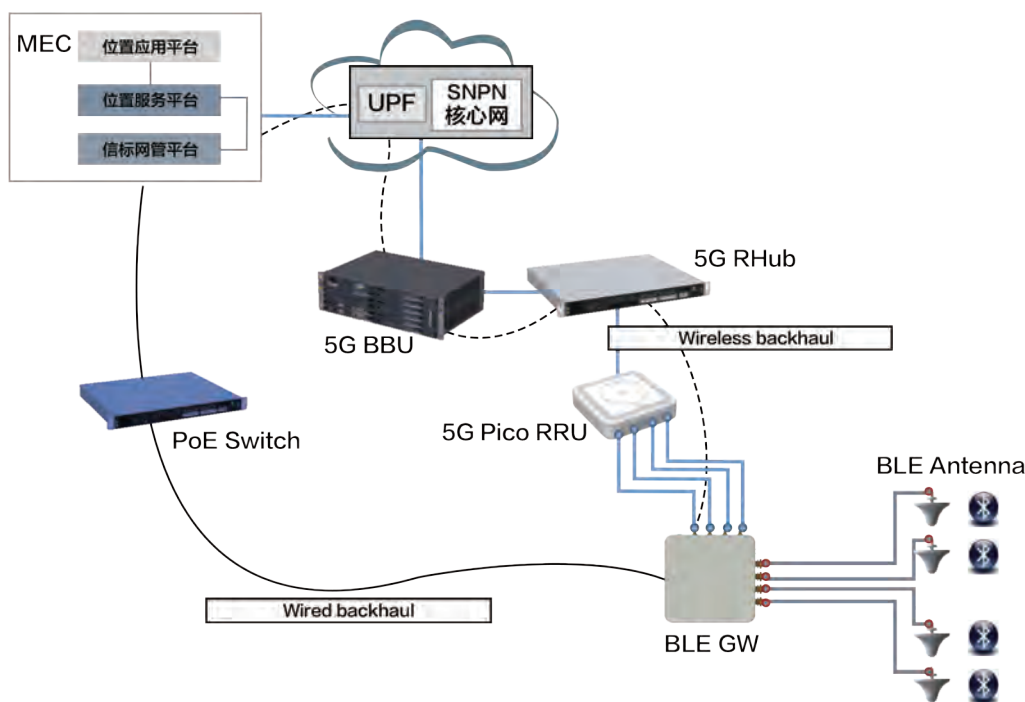


图 13 基于 BLE 的室内定位系统与 5G 融合部署方案

其中：

- 无线部分包括 5G 基站 BBU（BaseBand Unit，基带单元）、Pico RRU、RHub、室分天线、蓝牙网关和蓝牙信标。通过外接室分天线扩展 pRRU 的覆盖范围，降低室内 Pico RRU 单独组网的部署成本，Pico RRU 可以通过具备通直流能力的功分器外接多副室分天线；室分天线内置蓝牙信标，Pico RRU 外部集成蓝牙网关，一方面对于室分天线内置蓝牙信标进行供电，另一方面实现监控室分天线工作状态、配置蓝牙信标状态参数等功能。

- 位置应用平台、位置服务平台和蓝牙网管平台部署在 MEC 平台上，蓝牙网关采用无线或有线回传方案，与蓝牙网管平台连接，定位应用通过用户面数据连接获取位置信息和应用内容。

该方案提供高可用的基于蓝牙信标的室内位置服务，具备一定的成本优势，适合于规模化建设，室内定位精度可以达到 3 米左右。



5G 专网关键网络产品

5G 专网关键网络产品

5G 专网核心网有别于 5G 公网核心网。5G 公网核心网软件功能非常庞大且复杂，因此技术门槛高、价格昂贵。而 5G 专网需要的是低成本的、定制化的和功能要求相对简单的轻量化核心网。

5G 专网核心网的低成本和轻量化可以通过对公网核心网的网元功能进行裁剪和合设实现，如图 14 所示。通过裁剪掉不必要的网元功能，以及将功能相近、流程联系紧密的网元通过网元合设使网元外部接口通信变成内部消息，节省系统内存资源和计算资源开销。



图 14 轻量化核心网

5G 专网核心网的定制化主要面向 UPF。工业环境下的 UPF 除了能够做到基本的会话管理、数据转发、基本的 QoS 执行外，还需要按需支持工业以太网协议、确定性网络等定制功能，如图 15 所示。在产品形态上，也需要支持增配硬件加速卡，以应对转发数据量特别大的应用场景。此外，UPF 与 MEC 也有一体化的需求，以降低对机房配套条件的要求。

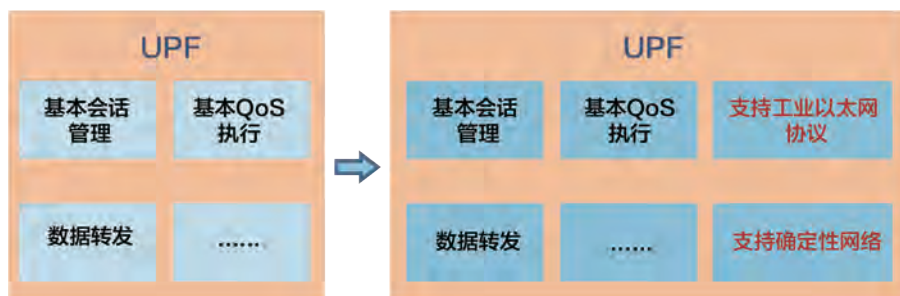
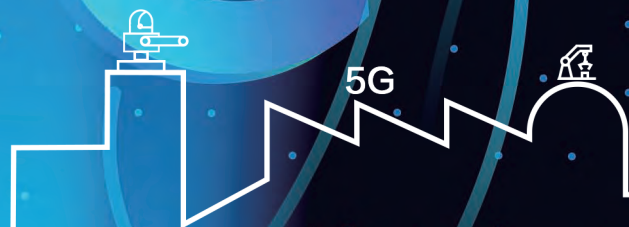


图 15 UPF 定制化

5G

结束语



结束语

2020年3月，中央提出要加快新型基础设施建设进度，以5G、人工智能、工业互联网、物联网为代表的新基建成为我国的战略发展方向。在该背景下，本白皮书提出面向工业互联网园区的5G专网技术方案；其核心内容是基于SA架构进行5G专网建设且专网专用，满足工业互联网园区多样化需求的同时，保证专网的高可用性、高可靠性和高安全性。在网络建设方面，采用宏站、微/杆站、室分站协同的方式，实现工业互联网园区的无线覆盖；通过网络切片方式，将工业互联网园区的工业生产网、企业信息网和公共服务网进行安全隔离，并确保工业生产网多场景业务并发下的性能保障；通过5G与TSN技术无缝融合，取代传统TSN网络有线传输方式，加速CT与工业IT及OT网络的融合进程；通过5G网络与基于BLE的室内定位系统融合部署，满足工业场景的高精准定位和室内外一体化的无缝定位要求。

展望未来工业互联网园区的5G专网建设，面临的主要问题有两个：

- **专网频谱是最大的问题。**国内目前无5G行业专用频段，预计行业5G频率获取时间长、难度大。而采用运营商为行业用户分配授权频谱中的独占频段的方式进行5G独立专网建设，目前国内尚无成功的商业模式。值得注意的是，近期国内已有部分先进省份开始申请相关频段，用于5G专网试点，这将使5G专网工作向前迈出一大步。此外，2018年底，3GPP批准了5G NR-U（5G NR in Unlicensed Spectrum，工作于非授权频谱的5G NR）项目工作，意味着垂直行业可以使用非授权频谱，以Stand-alone NR-U（独立NR-U）的方式自行部署独立的5G专网。随着未来5G专网的广泛部署，NR-U也将会有更多的使用场景和机会。

- **5G行业终端为瓶颈所在。**当前的行业终端主要采用CPE，未来随着5G产业的发展，行业终端需要通过集成5G通用模组等方式支持5G，并在速率、功耗、体积、成本等方面进一步优化。同时，需要针对差异化的垂直行业需求定制终端能力，如按需支持授时、TSN、eSIM、安全芯片等能力。因此，行业终端将会以5G通用模组+定制能力的形式广泛应用于未来的5G专网建设中。

共绘生态蓝图



官方微信



官方微博